Creating Smart Systems to Prevent Terrorism

Eytan Mottes
Vice-President of Business Development and U.S. Representative for Nezer Information Systems

CONTENT

INTRODUCTION

Nezer Information Systems is an international access control consulting firm, specializing in biometrics, smart cards, and border control. Nezer was chosen by several Israeli governmental agencies to coordinate, define, supervise, and execute the project of rebuilding the entire Israeli border control system.

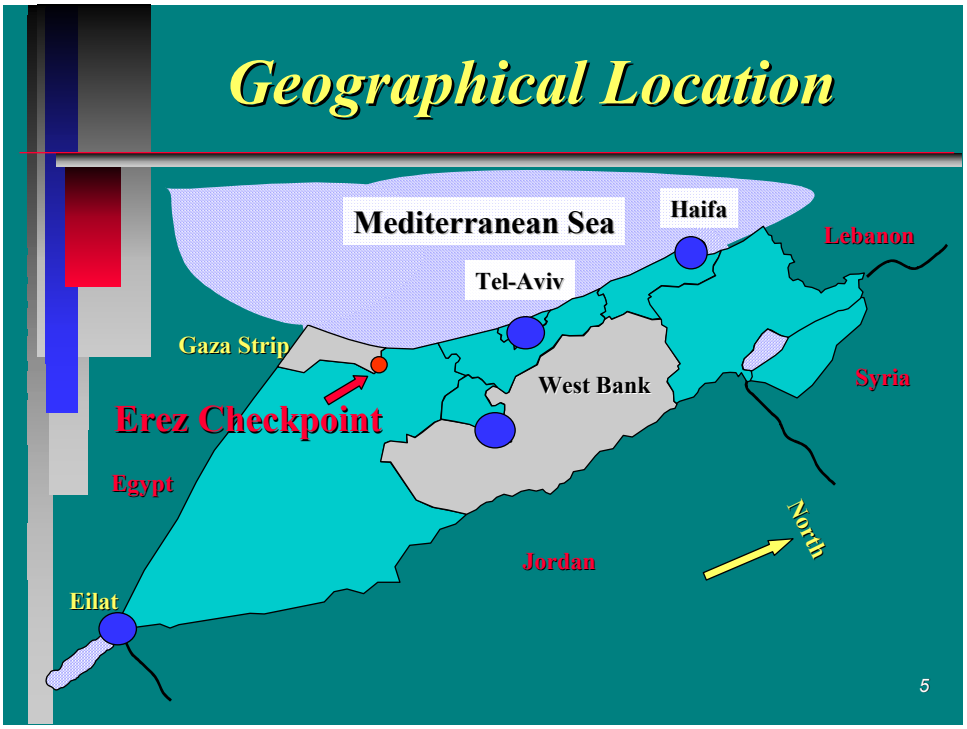
I am going to concentrate on the system that is going to be implemented at the Erez checkpoint. It is just one out of twenty-nine sites included in this project. However, let me begin with some words of caution:

- No single answer is suitable for all applications.
- One should carefully define his specific system requirements and constraints and design his own specific solution accordingly.

I will discuss a specific application with extreme constraints. Our conclusions are not necessarily a recommendation for any other application. Yet, the way we managed our own decision process should be a guide to other projects in this field.

GEOGRAPHICAL LOCATION

For your orientation, Erez is located north of the Gaza Strip. Erez has land borders with Egypt, Jordan, Syria, and Lebanon. The seaports are in the Mediterranean Sea and in the Red Sea. There are several international airports.



EREZ CHECKPOINT CHARACTERISTICS

Erez checkpoint is characterized by the following:

- Eighty thousand crossings a day, 365 days a year,
- Fifteen thousand people an hour,
- Two peak times a day, three hours each, one in the early morning and one in the afternoon,
- The population is permanent,
- Usually daily workers, mostly manual workers in construction, agriculture, restaurants, etc.

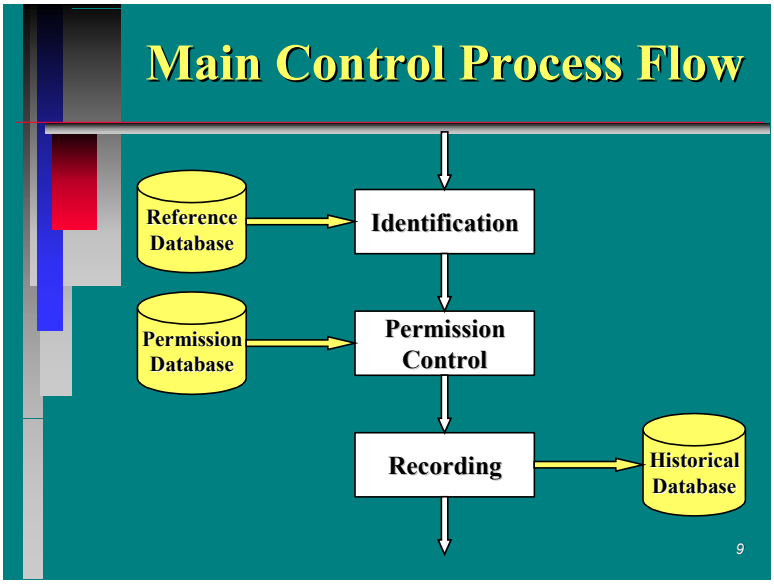
Additional characteristics include passengers that are part of humanitarian aid, VIP's, media teams, and other people who are not part of the regular and permanent population. Bear in mind, unlike most international borders, this is not a peaceful border. These are two communities in conflict. Security tension and alertness exist, but vary according to political situations and terrorist activities.

Major Functions of any Border Control

The major functions of any border control are:

- ID verification: Verifying that the inspected person is the one he claims to be.
- Eligibility control: Verifying that the person has the transit documents that allow him to enter or exit and there is no reason to prevent him from doing so.
- Recording: Writing the crossing event data to the historical database.

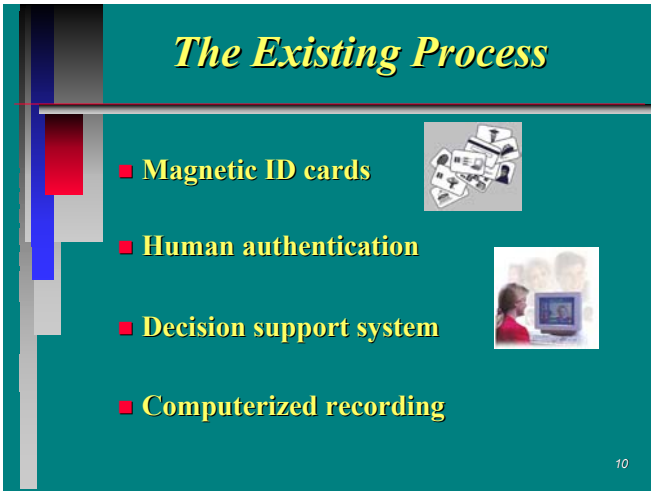
Main Control Process Flow



The process begins when a person approaches the inspection bar. The first step is to identify the person. This is done with the person's transit documents and is matched using a reference database, such as the population census or the national vehicle registry (if the passage is within a vehicle). The second step is to verify that the person is allowed to enter or exit the country. This is done versus a qualification database from the immigration, security, and custom authorities. The third and last step is to record the passage event into a historical database.

THE EXISTING SYSTEM

A system has already been established in which identification is verified using magnetic ID cards. Verification is done manually, by comparing the person's face with his or her image, which is stored in the system. Permission is granted based on a decision support system. Recording is done automatically.



NEW SYSTEM OBJECTIVES

The new system objectives are:

- Security improvements - to ensure that the person inspected is the person he claims to be and is authorized to enter or exit.
- Throughput increase - let more people cross in less time.
- Better service with self-dignity - speed up the process, shorten the waiting lines, and improve privacy and self-respect.
- Reduction of human friction - Let less human inspectors argue with the people in transit.
- Resource savings - Use fewer personnel in each shift to run the checkpoint.

Requirements Uniqueness

What makes the Erez checkpoint so unique?

In each security system, the crucial point is to evaluate the threat and adjust the means accordingly.

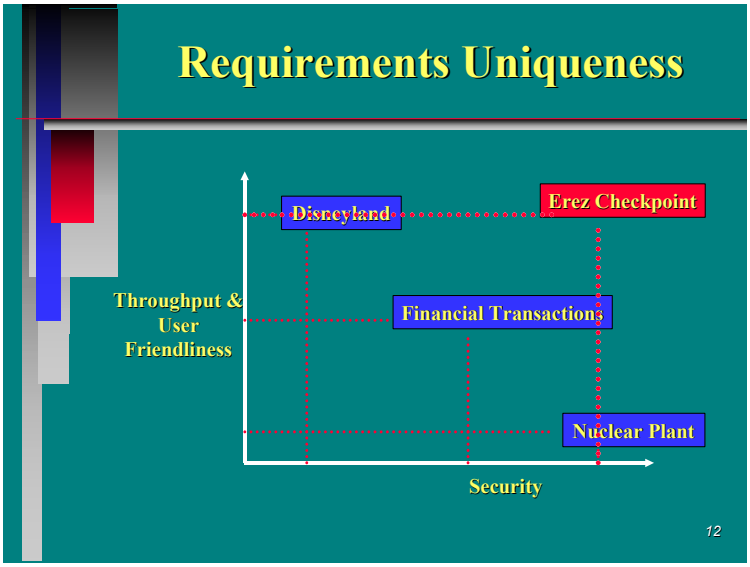
Usually access control is characterized by two kinds of demands that seem to be contradicting:

1. Throughput and user friendliness, and
2. Security and integrity of the process.

Disneyland access control may represent those cases that require a very high level of throughput and friendliness.

A nuclear plant may represent a relaxed throughput requirement, but much higher security level.

Financial transactions are an example of an application where one should find a compromise between user friendliness and security.



In most border control checkpoints, the risks are drug trafficking, illegal immigration, smuggling, and pornography, as is the case in the passage between Singapore and Malaysia.

In our case, the threat is of a terrorist carrying a bomb that might be exploded at the center of Tel-Aviv in one hour. Security cannot be compromised, yet the people need to cross fast and easy.

Solution Concept

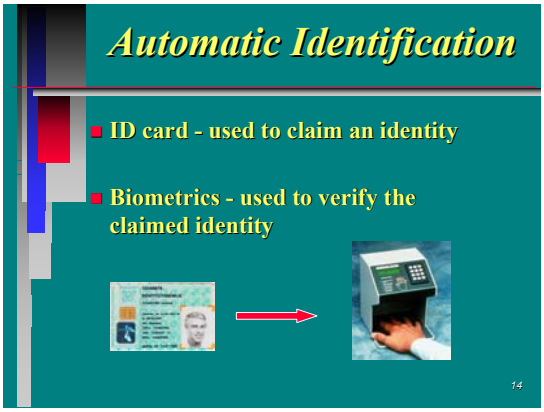
The concept of the new system design is based on automation:

- Automatic identification,
- Automatic permission control,
- Automatic recording and,
- Automatic transit gateways.

Automatic Identification

The first step in the process is the automatic person identification and verification.

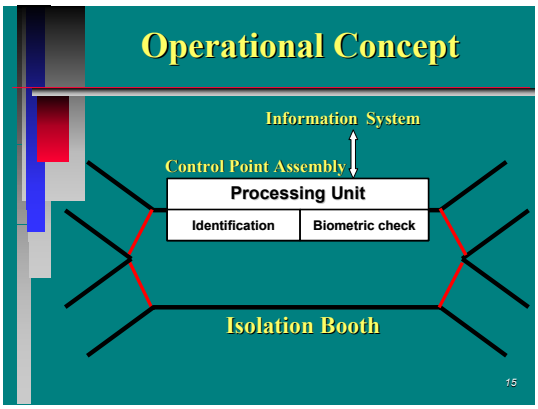
- An ID card is used as a means of claiming an identity.
- Biometrics is used to verify the claimed identity. That means that the requirement from the biometric technology is for a one-to-one check, as opposed to a one-to-many search.



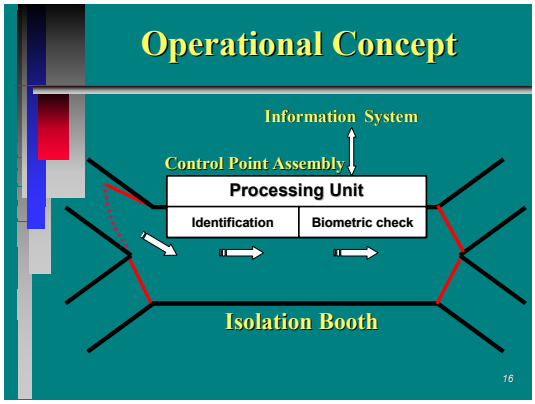
OPERATIONAL CONCEPT

This is a simplified model of the controlled passage. The passage is based on a booth with sensors to ensure that there is no more than one person at a time in the booth.

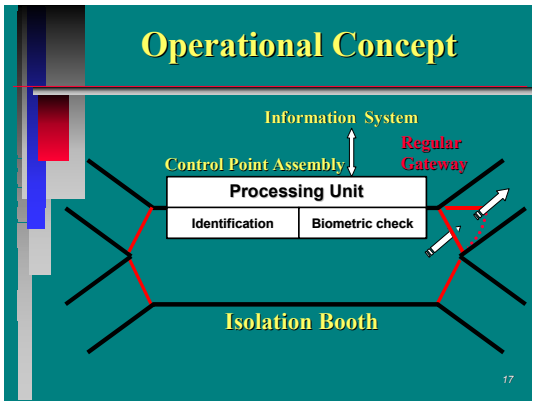
In the booth, there is a control assembly with an identification module and a biometric module. The control assembly communicates with the information system that holds the reference databases.



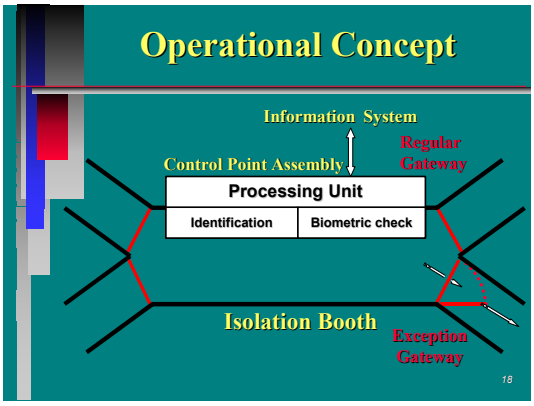
The person goes from left to right. When he enters, the entrance gate is closed and the booth is isolated until one of the exit gates is closed behind the exiting passenger.



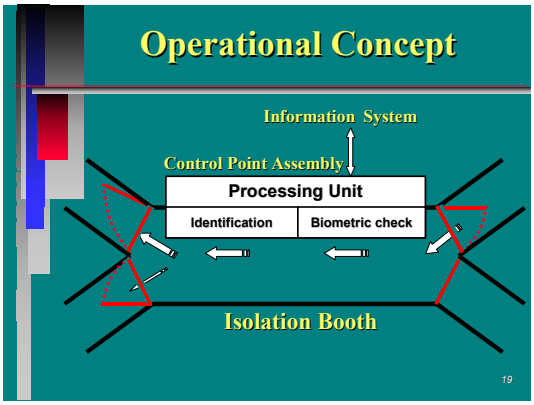
If everything is deemed acceptable, then the person exits the booth through the regular exit gateway.



If there is a problem, the person is then directed to the exception gateway to continue the process with a human inspection. (After that person exits, the relevant gate is closed and the next person can enter.)



The passage is bi-directional and can be switched to the other side to serve both directions - entry and exit from Israel.



Throughput Planning

Throughput planning is based upon 42 parallel gates. Each gate is bi-directional. Of the 42 gates, 10 will be multifunctional. The manned gates will accommodate VIP's, passengers that are not part of the permanent population, and passengers without a biometric enrollment. The gates will be managed according to the traffic.

In order to meet the throughput requirements of the peak times, a total of 9 to 12 seconds per person will be allowed in the automatic process. This time frame is essential for each passage; from opening the entry gate to the next opening of the entry gate, and it includes the human part of the process done by the passenger.

BIOMETRIC CRITERIA

The biggest uncertainty was deciding which biometric technology to use. First, the criteria had to be defined to determine how the technology would be evaluated before a decision was made.

The criteria, upon which the biometric technology should be evaluated, are, in decreasing order of importance:

1. The reliability of the technology was considered as the critical factor, but not a sufficient one.

2. Operational efficiency and convenience means the level of active involvement of the passenger and the time it takes. Does it require putting a hand or finger in any reading device or standing still in a certain pose? Flexibility means the ability to change the system's sensitivity according to different alert levels.

3. The biometrics technology should deal with people with wiped-out fingerprints, bruises and cuts, hands affected by chemicals and detergents, bearded men, sunglasses, and veiled women. The technology should also deal with the irregular population — handicapped people or people with permanent disabilities.

4. There are extreme conditions of heat, humidity, and dust storms in the Erez checkpoint.

5. Complexity of the enrolment process — the process in which the personal biometrics signature (such as face image, fingerprints, or hand geometry) is acquired and registered into the system database.

6. The last criterion is the technological maturity and proven experience.

Cost was the least significant factor in this system. If each passenger is charged a very small passage fee, the investment will be returned in a short period.

Biometric Reliability

The reliability of a biometric product is specified by the terms FAR, FRR, EFR:

- FAR - False Acceptance Rate. A higher rate is an indication that more people that should not pass will pass. A false acceptance is considered a security failure.

- FRR - False Rejection Rate. A higher rate is an indication that more qualified "honest" people will be rejected. A false rejection is considered an operational failure that creates stress in the waiting lines and on the human inspectors. Within that context, failure to acquire is also considered as a false rejection.

- The EFR - Equal False Rate. The point in which the two false rates are balanced.

Common acceptable failure rates fall between 1 percent to .1 percent, and most of the products available in the market are equipped with technical references that quote this level of figures.

Since the reliability had been defined as the most uncertain and critical factor and there was no neutral reference data available, the suppliers' statements were questionable. It was decided to conduct a field test or a benchmark within the bid process.

Reliability Benchmark

In June 1988, we conducted a controlled benchmark in a military base that involved:

- Eleven suppliers with twenty test stations
- Thirteen different products. Some products were tested in more then one station.
- The products represented six distinct biometric technologies plus one combination of two technologies:
    - Fingerprints, face recognition, palm geometry, iris, two-finger geometry, and voice. The combination was based on hand geometry with face recognition. You can assume that almost all the relevant important products in the market were involved in that benchmark.
- The test population consisted of 560 people, men and women, most of them about eighteen years old, each one with one enrollment and five to six test cycles.
- That sample gave us approximately 3,000 test samples for each test station, or 60,000 samples altogether.

Benchmark Targets

For the benchmark process, two principal thresholds were defined:

1. The first threshold was the initial minimal reliability rate. Any single product that does not meet this rate will be eliminated from the bid process. The minimal thresholds were that the false acceptance rate should be less than 1 percent and the false rejection rate should be less than 3 percent.

2. The second threshold was the target reliability rate. Final target rates were announced so that bidders would be able to balance and fine-tune their systems accordingly. The announced targeted thresholds were that the false acceptance rates and the false rejection rates should each be less than .1 percent.

Benchmark Process

The benchmark process was conducted according to the following rules:

- Identical process and conditions for all participants
- Unlimited enrolment tries
- A single try for each test sample.
- Up to 2 seconds for pass-fail decision.
- Benchmark organizers had full control of the participant's claimed identity, so that each person in each test cycle, came to the test stations and presented the ID number given by management. At times, the "real" ID was used, as the participant had been enrolled earlier. Those are considered "real" samples. In other cycles, false ID's were used. Those are considered "impersonate" samples.
- Using that system, about 20 percent of all the samples were of "real" tests and about 80 percent were of "impersonate" test samples. This ratio was the result of statistical planning to achieve a high level of confidence.

Main Benchmark Results

As suspected, and with a definite contrast to the manufacturers' claim, no single product met the targeted rates. Additionally, only two single products met the minimal, more relaxed rates.

The main conclusion was that there are many holes in the cheese.

There are many theories prevalent in the market about the relative reliability of each technology. I am not allowed to publish the test results of each product, but I can tell you that the two products that passed the minimal rates belong to the fingerprint and palm geometry technologies.

I have an unhappy hypothesis about the state of the biometrics industry and its customers. We are all in a kind of euphoria. That euphoria may be what is known as the "Titanic Syndrome." It was so big and safe that there was no need for rescue boats.

Additional Benchmark Results

Additional lessons learned from the analysis of the benchmark results:

- Of the twenty test stations, twelve have succeeded to enroll all the sample population. This is in opposition to some known theories that indicate that about 2 to 3 percent of the population in each technology, are unable to enroll at all.

- There were variations between test results of the same product in different test stations**.** As I have mentioned earlier, there were some test stations with the same product. This may be the result of human intervention (the participants, the station operators, and the technicians who tuned the products.)

- An insignificant learning curve has been found in only four test stations, and no learning curve at any of the other stations. Let me make clear that each participant was enrolled in the morning. They were then tested five to six times during the same day, with approximately a two-hour span between each cycle. All of them were young people about the same age. There are theories and some statistical data, which claim that there is a significant learning curve along the time of using a biometric system.

- It has been observed that all the operators of the fingerprint products kept cleaning their readers during the course of the benchmark. This phenomenon has an important impact on operational considerations.

MAIN CONCLUSION

To summarize our conclusions of the benchmark results and analyses, it can be said that for our purposes, regarding reliability and operational flexibility, one biometric technology is not enough.

This conclusion has directed us to the use of two combined biometric methods simultaneously.

DERIVED CONCLUSIONS

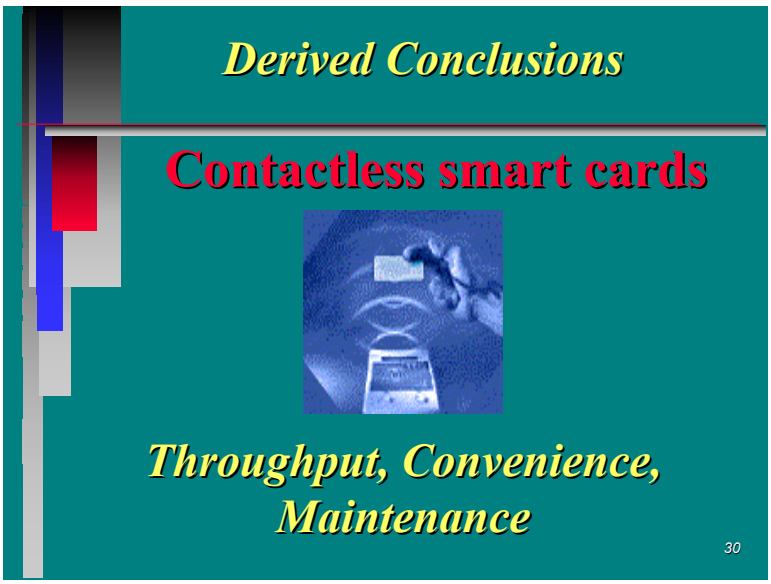
Yet, it is understood that this combination is not as trivial as it seems to be. One must make use of some fusion technique in order to achieve the advantages of using this kind of combination, and to overcome the inherent disadvantages associated with the naive "and/or" approach.

We own the know-how to do that and we will meet our reliability goals, even exceed them. Therefore, we can say that the reliability question is solved. Now throughput and convenience may become the bottleneck.

When considering the human passenger involvement and throughput issues, precedence is given to passive technologies as opposed to active ones. We cannot afford both technologies to be active; for example, that the person will have to put his finger **and** his hand in two separate readers. At least one biometric technology must be a passive one.

The optimal solution for our purposes was found to be the combination of palm geometry and face recognition. This combination gives us the benefits of high reliability, high throughput, flexibility, simplicity, convenience, no criminal or irritating image, the ability to deal with irregular population, and a very high challenge to those who will try to cheat the system with artificial or dead organs.

For almost the same reasons — convenience, throughput, and simplicity, the contactless smart card, vis-à-vis the contact card, is preferred.



FINAL STATEMENT

I will conclude with the same statement as in the beginning of the discussion:

- No single answer is suitable for all applications.
- One should carefully define his specific system requirements and constraints, and design his own specific solution accordingly.

EYTAN MOTTES

Eytan Mottes is Vice President of Business Development, U.S. Representative for NEZER, an integrator of biometrics security systems. He worked with IBM for more than 20 years in Europe, Israel and the U.S., in management of marketing and sales of IBM Enterprise Solutions. Consulted organization management in strategic planning and development of complex information and communication systems. Among his customers were Israeli security agencies, banks and various government departments, including the Israeli Ministry of Defense, Israeli Aircraft Industry and RAFAEL.

Eytan Mottes served in the Israel Defense Forces as Lt. Colonel, commanding the development of operational artillery field computer system. He lectured at the Technion in Haifa and other universities in Israel on information system development. He has a BSC in Mathematics from the Hebrew University of Jerusalem. He has many Certificates from IBM business schools in Business Administration, Project Management and Consulting.